

Inhaltsverzeichnis

Teil 1

Wozu Kryptografie?

1	Einleitung	3
1.1	Kryptografie heute.	4
1.2	Die sechste Ausgabe	5
1.2.1	Erste Ausgabe (1998)	5
1.2.2	Zweite Ausgabe (2001)	5
1.2.3	Dritte Ausgabe (2007)	5
1.2.4	Vierte Ausgabe (2009)	6
1.2.5	Fünfte Ausgabe (2013)	6
1.2.6	Sechste Ausgabe (2015)	6
1.3	Mein Bedauern, meine Bitten und mein Dank	7
2	Was ist Kryptografie und warum ist sie so wichtig?	9
2.1	The Name of the Game	9
2.1.1	Die kurze Antwort	9
2.1.2	Die lange Antwort.	9
2.2	Die Kryptografie – ein wichtiges Teilgebiet	11
2.3	Warum ist die Kryptografie so wichtig?	12
2.3.1	Wirtschaftsspionage	13
2.3.2	Kommerz im Netz	13
2.3.3	Die Privatsphäre	13
2.3.4	Technik und Infrastrukturen	14
2.4	Anwendungen der Kryptografie.	14
2.5	Und wer zum Teufel ist Alice?	15

3	Wie und vom wem Daten abgehört werden	17
3.1	Mallory am Übertragungsmedium	17
3.1.1	Kupferkabel	18
3.1.2	Glasfaser	18
3.1.3	Drahtlose Datenübertragung	19
3.1.4	Satellit	19
3.2	Mallory am Gerät	19
3.2.1	Netzkomponenten	20
3.2.2	Mitlesen und Verändern von Dateien	20
3.3	Mallory in Computernetzen	20
3.3.1	Telefon	20
3.3.2	LAN	21
3.3.3	DSL	22
3.3.4	Mobilfunk	22
3.3.5	WLANs	23
3.4	Mallory im Internet	23
3.4.1	ARP-Spoofing	23
3.4.2	Abhörangriffe auf Router	24
3.4.3	IP-Spoofing	24
3.4.4	DNS-Spoofing	25
3.4.5	Mitlesen von E-Mails	26
3.4.6	URL-Spoofing	27
3.4.7	Abhören von Internettelefonie	27
3.5	Ein paar Fälle aus der Praxis	27
3.5.1	Mitgelesene E-Mails	28
3.5.2	Abgehörte Telefonate	29
3.6	Ist Kryptografie gefährlich?	30
3.6.1	Nachteile einer Krypto-Beschränkung	32
3.6.2	Vorteile einer Krypto-Beschränkung	33
3.6.3	Fazit	36
4	Klassische symmetrische Verschlüsselung	39
4.1	Symmetrische Verschlüsselung	39
4.1.1	Kryptografische Fachbegriffe	41
4.1.2	Angriffe auf Verschlüsselungsverfahren	41
4.2	Monoalphabetische Substitutionschiffren	42
4.2.1	Caesar-Chiffre	43
4.2.2	Freie Buchstabensubstitution	44
4.2.3	Homophone Chiffre	45

4.2.4	Bigramm-Substitution	47
4.2.5	Playfair-Chiffre	48
4.2.6	Nomenklatoren und Wörter-Codes	49
4.3	Polyalphabetische Substitutionschiffren	50
4.3.1	Vigenère-Chiffre	50
4.3.2	Vernam-Chiffre	51
4.3.3	One-Time-Pad	52
4.4	Permutationschiffren	53
4.4.1	Kryptoanalyse von Permutationschiffren	54
4.4.2	Bedeutung von Permutationschiffren	55
4.5	Berühmte ungelöste Verschlüsselungen	56
4.5.1	Das Voynich-Manuskript	57
4.5.2	Der Zettel des Somerton-Manns	57
4.5.3	Das Thouless-Kryptogramm	58
4.5.4	Weitere ungelöste Rätsel	59
5	Die Enigma und andere Verschlüsselungsmaschinen	61
5.1	Verschlüsselungswerkzeuge	62
5.2	Rotorchiffren	65
5.2.1	Heberns Rotormaschine	65
5.2.2	Die Enigma	66
5.2.3	Weitere Rotor-Chiffriermaschinen	70
5.3	Weitere Verschlüsselungsmaschinen	71
5.3.1	Die Kryha-Maschine	71
5.3.2	Hagelin-Maschinen	73
5.3.3	Die Purple	75
5.3.4	Der Geheimschreiber	77
5.3.5	Die Lorenz-Maschine	79
5.3.6	Schlüsselgerät 41 (Hitler-Mühle)	80

Teil 2

Moderne Kryptografie

6	Der Data Encryption Standard	85
6.1	DES-Grundlagen	85
6.2	Funktionsweise des DES	88
6.2.1	Die Rundenfunktion F	89
6.2.2	Die Schlüsselaufbereitung des DES	90
6.2.3	Entschlüsseln mit dem DES	91

6.3	Sicherheit des DES	91
6.3.1	Vollständige Schlüsselsuche	91
6.3.2	Differenzielle und lineare Kryptoanalyse	92
6.3.3	Schwache Schlüssel	93
6.4	Triple-DES	94
6.4.1	Doppel-DES	94
6.4.2	Triple-DES	95
6.5	DES-Fazit	96
7	Chiffren-Design	97
7.1	Sicherheitsüberlegungen	98
7.1.1	Mögliche Schwachstellen	98
7.1.2	Sicherheit gegenüber speziellen Angriffen	100
7.1.3	Die ideale Schlüssellänge	101
7.1.4	Hintertüren	103
7.2	Weitere Designkriterien	105
7.3	Aufbau symmetrischer Verschlüsselungsverfahren	105
7.3.1	Linearität	107
7.3.2	Konfusion und Diffusion	108
7.3.3	Rundenprinzip	109
7.3.4	Schlüsselaufbereitung	111
8	Kryptoanalyse symmetrischer Verfahren	113
8.1	Differenzielle Kryptoanalyse	114
8.2	Lineare Kryptoanalyse	118
8.3	Kryptoanalyse mit Quantencomputern	120
8.4	Weitere Kryptoanalyse-Methoden	120
9	Symmetrische Verfahren, die vor dem AES entstanden sind	123
9.1	RC2 und RC5	123
9.1.1	RC2	124
9.1.2	RC5	126
9.2	Blowfish	128
9.2.1	Funktionsweise von Blowfish	129
9.2.2	Schlüsselaufbereitung von Blowfish	129
9.2.3	Bewertung von Blowfish	130
9.3	IDEA und IDEA NXT	131
9.4	Skipjack	132
9.5	TEA	133
9.6	GOST	134
9.7	Weitere symmetrische Verfahren	135

10	Der Advanced Encryption Standard (AES)	137
10.1	Funktionsweise des AES	138
10.1.1	Rundenaufbau	139
10.1.2	Entschlüsselung mit dem AES	142
10.1.3	Schlüsselaufbereitung	142
10.2	Mathematische Betrachtung des AES	144
10.3	Sicherheit des AES	145
10.3.1	AES als algebraische Formel	146
10.3.2	Quadratische Kryptoanalyse	147
10.3.3	Biclique-Kryptoanalyse	148
10.3.4	Weitere Angriffe	148
10.4	Bewertung des AES	148
11	AES-Kandidaten	151
11.1	Serpent	151
11.1.1	Funktionsweise von Serpent	152
11.1.2	S-Box-Design	153
11.1.3	Schlüsselaufbereitung von Serpent	154
11.1.4	Bewertung von Serpent	155
11.2	Twofish	155
11.2.1	Funktionsweise von Twofish	156
11.2.2	Bewertung von Twofish	157
11.3	RC6	157
11.3.1	Funktionsweise von RC6	158
11.3.2	Schlüsselaufbereitung von RC6	159
11.3.3	Bewertung von RC6	160
11.4	MARS	160
11.5	SAFER	162
11.5.1	Funktionsweise von SAFER+	162
11.5.2	Schlüsselaufbereitung von SAFER+	164
11.5.3	Bewertung von SAFER+	165
11.6	CAST	165
11.7	MAGENTA	166
11.8	Die restlichen AES-Kandidaten	168
11.9	Fazit	169

12	Symmetrische Verfahren, die nach dem AES entstanden sind	171
12.1	MISTY1, KASUMI und Camellia	171
12.1.1	MISTY1	172
12.1.2	KASUMI	173
12.1.3	Camellia	174
12.2	Chiasmus und Libelle	175
12.2.1	Funktionsweise von Chiasmus	175
12.2.2	Libelle	176
12.3	CLEFIA	176
12.3.1	Funktionsweise von CLEFIA	177
12.3.2	Bewertung von CLEFIA	178
12.4	Schlanke Verschlüsselungsverfahren	178
12.4.1	SEA	180
12.4.2	PRESENT	182
12.4.3	Bewertung schlanker Verfahren	183
12.5	Tweak-Verfahren	184
12.5.1	Beispiele	184
12.5.2	Threefish	185
12.5.3	Bewertung von Tweak-Verfahren	187
12.6	Weitere symmetrische Verschlüsselungsverfahren	187
13	Asymmetrische Verschlüsselung	189
13.1	Ein bisschen Mathematik	192
13.1.1	Modulo-Rechnen	192
13.1.2	Einwegfunktionen und Falltürfunktionen	198
13.2	Der Diffie-Hellman-Schlüsselaustausch	199
13.2.1	Funktionsweise von Diffie-Hellman	200
13.2.2	MQV	202
13.3	RSA	204
13.3.1	Funktionsweise des RSA-Verfahrens	204
13.3.2	Ein Beispiel	206
13.3.3	Sicherheit des RSA-Verfahrens	206
13.3.4	RSA und der Chinesische Restsatz	210
13.4	Symmetrisch und asymmetrisch im Zusammenspiel	213
13.4.1	Unterschiede zwischen symmetrisch und asymmetrisch	213
13.4.2	Hybridverfahren	214

14	Digitale Signaturen	215
14.1	Was ist eine digitale Signatur?	216
14.2	RSA als Signaturverfahren	217
14.2.1	Funktionsweise	217
14.2.2	Sicherheit von RSA-Signaturen	217
14.3	Signaturen auf Basis des diskreten Logarithmus	218
14.3.1	ElGamal-Verfahren	219
14.3.2	DSA	220
14.3.3	Weitere DLSSs.	223
14.4	Unterschiede zwischen DLSSs und RSA.	223
14.5	Weitere Signatur-Verfahren	224
15	Weitere asymmetrische Krypto-Verfahren	225
15.1	Krypto-Systeme auf Basis elliptischer Kurven	226
15.1.1	Elliptische Kurven	226
15.1.2	ECC-Verfahren	228
15.1.3	Die wichtigsten ECC-Verfahren	229
15.1.4	Beispiel-Kurven	230
15.1.5	Montgomery- und Edwards-Kurven	230
15.2	NTRU	232
15.2.1	Mathematische Grundlagen	232
15.2.2	Funktionsweise von NTRU	232
15.2.3	Bewertung von NTRU.	234
15.3	XTR	234
15.4	Krypto-Systeme auf Basis hyperelliptischer Kurven	235
15.5	HFE.	235
15.5.1	Mathematische Grundlagen	236
15.5.2	Das Verfahren.	236
15.5.3	Bewertung von HFE	237
15.6	McEliece-Verfahren.	238
15.7	Weitere asymmetrische Verfahren	239
16	Kryptografische Hashfunktionen	241
16.1	Was ist eine kryptografische Hashfunktion?	242
16.1.1	Nichtkryptografische Hashfunktionen	242
16.1.2	Kryptografische Hashfunktionen.	243
16.1.3	Angriffe auf kryptografische Hashfunktionen	244
16.2	SHA-1	252
16.2.1	Funktionsweise von SHA-1	252
16.2.2	Bewertung von SHA-1.	255

16.3	SHA-2	256
16.3.1	SHA-256	256
16.3.2	SHA-224	257
16.3.3	SHA-512	258
16.3.4	SHA-384	258
16.3.5	SHA-512/224 und SHA-512/256	258
16.3.6	Bewertung von SHA-2	258
16.4	MD4	259
16.5	MD5	259
16.6	RIPEMD-160	260
16.6.1	Funktionsweise von RIPEMD-160	261
16.6.2	Bewertung von RIPEMD-160	263
17	Weitere kryptografische Hashfunktionen	265
17.1	Tiger	265
17.1.1	Funktionsweise von Tiger	266
17.1.2	Bewertung von Tiger	268
17.2	WHIRLPOOL	268
17.2.1	Funktionsweise von WHIRLPOOL	269
17.2.2	Das Verschlüsselungsverfahren W	269
17.2.3	Bewertung von WHIRLPOOL	270
17.3	SHA-3 (Keccak)	271
17.3.1	Funktionsweise von Keccak	273
17.4	Hashfunktionen aus Verschlüsselungsverfahren	276
17.4.1	Variante 1	277
17.4.2	Variante 2	277
17.4.3	Variante 3 und 4	278
17.4.4	Fazit	278
17.5	Hashfunktionen aus Tweak-Verfahren	279
17.6	Weitere kryptografische Hashfunktionen	279
18	Weitere Anwendungen kryptografischer Hashfunktionen	281
18.1	Schlüsselabhängige Hashfunktionen	281
18.1.1	Anwendungsbereiche schlüsselabhängiger Hashfunktionen	282
18.1.2	Die wichtigsten schlüsselabhängigen Hashfunktionen	283
18.1.3	Fazit	285
18.2	Hashbäume	285
18.3	Hash-Signaturverfahren	286
18.3.1	Lamport-Diffie-Einmal-Signaturverfahren	287
18.3.2	Merkle-Signaturverfahren	287
18.3.3	Bewertung von Hash-Signaturverfahren	288

18.4	Künstliche Verzögerungen durch Hashfunktionen	289
18.5	Weitere Anwendungen kryptografischer Hashfunktionen	290
19	Kryptografische Zufallsgeneratoren	293
19.1	Zufallszahlen in der Kryptografie	294
19.1.1	Anforderungen der Kryptografie	294
19.1.2	Echte Zufallsgeneratoren.	295
19.1.3	Pseudozufallsgeneratoren	296
19.1.4	Die Grauzone zwischen echt und pseudo.	297
19.1.5	Mischen von Zufallsquellen	297
19.2	Die wichtigsten Pseudozufallsgeneratoren	298
19.2.1	Kryptografische Hashfunktionen als Fortschaltfunktion . . .	300
19.2.2	Schlüsselabhängige Hashfunktionen als Fortschaltfunktion. .	302
19.2.3	Blockchiffren als Fortschaltfunktion	304
19.2.4	Linear rückgekoppelte Schieberegister.	304
19.2.5	Nichtlinear rückgekoppelte Schieberegister	306
19.2.6	Zahlentheoretische Pseudozufallsgeneratoren	307
19.3	Primzahlgeneratoren	308
20	Kryptoanalyse mit Quantencomputern und Post-Quanten-Kryptografie	311
20.1	Quantenmechanik	312
20.1.1	Superpositionen.	312
20.1.2	Verschränkungen	313
20.2	Quantencomputer	313
20.3	Faktorisierung mit dem Shor-Algorithmus.	315
20.4	Vollständige Schlüsselsuche mit dem Grover-Algorithmus.	315
20.5	Wie realistisch sind Quantencomputer	316
20.6	Post-Quanten-Kryptografie	317
21	Stromchiffren	319
21.1	Aufbau und Eigenschaften von Stromchiffren	320
21.1.1	Wie eine Stromchiffre funktioniert	321
21.1.2	Angriffe auf Stromchiffren	322
21.1.3	Stromchiffren und Blockchiffren im Vergleich.	322
21.2	RC4.	324
21.2.1	Funktionsweise von RC4.	324
21.2.2	Bewertung von RC4	325
21.3	A5	327
21.3.1	Funktionsweise von A5	327
21.3.2	Bewertung von A5.	328

21.4	E0	329
21.4.1	Funktionsweise von E0	329
21.4.2	Bewertung von E0	332
21.5	Crypto1	333
21.5.1	Funktionsweise von Crypto1	334
21.5.2	Bewertung von Crypto1	334
21.6	Die Verfahren des eSTREAM-Wettbewerbs	335
21.6.1	HC-128	336
21.6.2	Rabbit	338
21.6.3	Salsa20	342
21.6.4	Sosemanuk	344
21.6.5	Trivium	345
21.6.6	Grain	347
21.6.7	MICKEY	349
21.6.8	Erkenntnisse aus dem eSTREAM-Wettbewerb	351
21.7	Spritz	352
21.7.1	Funktionsweise von Spritz	352
21.7.2	Bewertung von Spritz	353
21.8	Snow 3G	353
21.8.1	Funktionsweise von Snow 3G	353
21.8.2	Bewertung von Snow 3G	355
21.9	Weitere Stromchiffren	355

Teil 3

Implementierung von Kryptografie

22	Real-World-Attacks	359
22.1	Seitenkanalangriffe	359
22.1.1	Zeitangriffe	360
22.1.2	Stromangriffe	362
22.1.3	Fehlerangriffe	364
22.1.4	Weitere Seitenkanalangriffe	365
22.2	Malware-Angriffe	365
22.2.1	Malware-Angriffe auf Schlüssel und Passwörter	366
22.2.2	Malware-Angriffe auf digitale Signaturen	367
22.2.3	Vom Entwickler eingebaute Hintertüren	369
22.2.4	Gegenmaßnahmen	370
22.3	Physikalische Angriffe	371
22.3.1	Die wichtigsten physikalischen Angriffe	371
22.3.2	Gegenmaßnahmen	372

22.4	Schwachstellen durch Implementierungsfehler	374
22.4.1	Implementierungsfehler in der Praxis	374
22.4.2	Implementierungsfehler in vielen Variationen	376
22.4.3	Gegenmaßnahmen.	377
22.5	Insiderangriffe	379
22.5.1	Unterschätzte Insider.	380
22.5.2	Gegenmaßnahmen.	380
22.6	Der Anwender als Schwachstelle	381
22.6.1	Schwachstellen durch Anwenderfehler	382
22.6.2	Gegenmaßnahmen.	384
22.7	Fazit	388
23	Standardisierung in der Kryptografie	389
23.1	Standards	389
23.1.1	Standardisierungsgremien	390
23.1.2	Standardisierung im Internet.	391
23.2	Wissenswertes zum Thema Standards	391
23.3	Wichtige Kryptografie-Standards.	392
23.3.1	PKCS.	392
23.3.2	IEEE P1363.	393
23.3.3	ANSI X.9	394
23.3.4	NSA Suite B	395
23.4	Standards für verschlüsselte und signierte Daten	396
23.4.1	PKCS#7.	396
23.4.2	XML Signature und XML Encryption.	398
23.4.3	Weitere Formate	400
23.5	Standardisierungswettbewerbe	400
23.5.1	Der DES-Wettbewerb	401
23.5.2	Der AES-Wettbewerb	402
23.5.3	Der SHA-3-Wettbewerb	405
23.5.4	Weitere Wettbewerbe	406
24	Betriebsarten und Datenformatierung	409
24.1	Betriebsarten von Blockchiffren.	409
24.1.1	Electronic-Codebook-Modus	410
24.1.2	Cipher-Block-Chaining-Modus	412
24.1.3	Output-Feedback-Modus	413
24.1.4	Cipher-Feedback-Modus.	414
24.1.5	Counter-Modus.	415
24.1.6	Fazit	417

24.2	Betriebsarten von Tweak-Verfahren	418
24.3	Formaterhaltende Verschlüsselung	419
24.4	Datenformatierung für das RSA-Verfahren.	419
24.4.1	Der PKCS#1-Standard	420
24.4.2	Datenformatierung für die RSA-Verschlüsselung	420
24.4.3	Datenformatierung für RSA-Signaturen	423
24.5	Datenformatierung für DLSSs.	425
25	Kryptografische Protokolle	427
25.1	Protokolle.	428
25.1.1	Konzeptprotokolle	428
25.1.2	Netzwerkprotokolle	429
25.1.3	Eigenschaften von Netzwerkprotokollen	430
25.2	Protokolle in der Kryptografie	432
25.2.1	Eigenschaften kryptografischer Netzwerkprotokolle	432
25.3	Angriffe auf kryptografische Protokolle	434
25.3.1	Replay-Attacke.	434
25.3.2	Spoofing-Attacke	435
25.3.3	Man-in-the-Middle-Attacke	435
25.3.4	Hijacking-Attacke	437
25.3.5	Known-Key-Attacken.	437
25.3.6	Verkehrsflussanalyse	440
25.3.7	Denial-of-Service-Attacke.	441
25.3.8	Sonstige Angriffe	442
25.4	Beispielprotokolle.	442
25.4.1	Beispielprotokoll: Messgerät sendet an PC	442
25.4.2	Weitere Beispielprotokolle	445
26	Authentifizierung	447
26.1	Authentifizierung im Überblick.	447
26.1.1	Etwas, was man weiß.	449
26.1.2	Was man hat	450
26.1.3	Was man ist	451
26.2	Biometrische Authentifizierung.	451
26.2.1	Grundsätzliches zur biometrischen Authentifizierung.	451
26.2.2	Biometrische Merkmale	453
26.2.3	Fazit.	457

26.3	Authentifizierung in Computernetzen	457
26.3.1	Passwörter	458
26.3.2	OTP-Tokens	461
26.3.3	Authentifizierung mit asymmetrischen Verfahren	464
26.3.4	Biometrie in Computernetzen	467
27	Verteilte Authentifizierung	469
27.1	Authentifizierungs-Synchronisation	470
27.2	Single Sign-on	470
27.2.1	Lokales SSO	471
27.2.2	Ticket-SSO	472
27.3	Kerberos	472
27.3.1	Vereinfachtes Kerberos-Protokoll	473
27.3.2	Vollständiges Kerberos-Protokoll	474
27.3.3	Vor- und Nachteile von Kerberos	476
27.4	RADIUS und andere Triple-A-Server	477
27.4.1	Triple-A-Server	477
27.4.2	Beispiele für Triple-A-Server	479
27.5	SAML	479
27.5.1	Funktionsweise von SAML	480
27.5.2	SAML in der Praxis	481
28	Krypto-Hardware und Krypto-Software	483
28.1	Krypto-Hardware oder Krypto-Software?	483
28.1.1	Pro Software	484
28.1.2	Pro Hardware	485
28.1.3	Ist Hardware oder Software besser?	485
28.2	Smartcards	486
28.2.1	Smartcards und andere Chipkarten	486
28.2.2	Smartcard-Formfaktoren	488
28.2.3	Smartcards und Kryptografie	489
28.3	Hardware-Security-Module	493
28.4	Kryptografie in eingebetteten Systemen	494
28.4.1	Eingebettete Systeme und Kryptografie	495
28.4.2	Kryptografische Herausforderungen in eingebetteten Systemen. 496	
28.5	RFID und Kryptografie	498
28.5.1	Sicherheitsprobleme beim Einsatz von EPC-Chips	499
28.5.2	RFID und Kryptografie	501

29	Management geheimer Schlüssel	505
29.1	Schlüsselgenerierung	506
29.2	Schlüsselspeicherung	508
29.3	Schlüsselauthentifizierung	509
29.4	Schlüsseltransport und Schlüssel-Backup	509
29.5	Schlüsselaufteilung	510
29.6	Schlüsselwechsel	511
29.7	Löschen eines Schlüssels	512
29.8	Key Recovery	512
29.9	Quantenkryptografie	513
29.9.1	Quanten-Schlüsselaustausch	513
29.9.2	Bewertung der Quantenkryptografie	515
30	Trusted Computing und Kryptografie	517
30.1	Trusted Computing	517
30.2	Trusted Computing und Kryptografie	519
30.3	Das Trusted Platform Module	519
30.3.1	Bestandteile des TPM	520
30.3.2	Schlüssel	521
30.4	Funktionen und Anwendungen des TPM	522
30.4.1	Fazit	523
31	Kryptografische APIs	525
31.1	PKCS#11	525
31.1.1	Aufbau	526
31.1.2	Rollenmodell	527
31.1.3	Prozesse	527
31.1.4	Bewertung von PKCS#11	528
31.2	MS-CAPI	529
31.2.1	Aufbau	529
31.2.2	Rollen	530
31.2.3	Prozesse	530
31.2.4	Bewertung der MS-CAPI	531
31.3	Cryptography API Next Generation (CNG)	531
31.4	TokenD	531
31.5	ISO/IEC 24727	532

31.6	Universelle Krypto-APIs	533
31.6.1	GSS-API und SSPI	533
31.6.2	CDSA	534
31.6.3	Krypto-APIs in Java	535
31.7	Weitere Krypto-APIs	536
32	Evaluierung und Zertifizierung	537
32.1	ITSEC	539
32.2	Common Criteria	541
32.3	FIPS 140	546
32.3.1	Die vier Stufen von FIPS 140.	547
32.3.2	Die Sicherheitsbereiche von FIPS 140	548
32.3.3	Bewertung von FIPS-140.....	555
32.4	Open Source als Alternative	555
32.4.1	Open Source	556
32.4.2	Beispiele	557
32.5	Fazit	558

Teil 4

Public-Key-Infrastrukturen

33	Public-Key-Infrastrukturen	561
33.1	Warum brauchen wir eine PKI?.....	561
33.1.1	Authentizität der Schlüssel	562
33.1.2	Sperrung von Schlüsseln	562
33.1.3	Verbindlichkeit	562
33.1.4	Durchsetzen einer Policy	562
33.2	Digitale Zertifikate	563
33.3	Vertrauensmodelle.....	565
33.3.1	Direct Trust.....	565
33.3.2	Web of Trust.....	566
33.3.3	Hierarchical Trust.....	567
33.3.4	PKI-Varianten.....	569
33.4	PKI-Standards	573
33.4.1	X.509	573
33.4.2	PKIX.....	573
33.4.3	Common PKI	574
33.4.4	OpenPGP	574

33.5	Aufbau und Funktionsweise einer PKI	575
33.5.1	Komponenten einer PKI	575
33.5.2	Rollen in einer PKI	582
33.5.3	Prozesse in einer PKI	583
33.6	Identitätsbasierte Krypto-Systeme	587
33.6.1	Funktionsweise	587
33.6.2	Das Boneh-Franklin-Verfahren	588
34	Digitale Zertifikate	591
34.1	X.509v1- und X.509v2-Zertifikate	591
34.1.1	Das Format	592
34.1.2	Nachteile von X.509v1 und v2	593
34.2	X.509v3-Zertifikate	593
34.2.1	Die X.509v3-Standarderweiterungen	594
34.3	Weitere X.509-Profile	596
34.3.1	Die PKIX-Erweiterungen	596
34.3.2	Die Common-PKI-Erweiterungen	597
34.3.3	Attribut-Zertifikate	598
34.3.4	X.509-Fazit	599
34.4	PGP-Zertifikate	599
34.4.1	OpenPGP-Pakete	599
34.4.2	PGP-Zertifikatsformat	601
34.4.3	Unterschiede zu X.509	603
34.5	CV-Zertifikate	603
35	PKI-Prozesse im Detail	607
35.1	Anwender-Enrollment	607
35.1.1	Schritt 1: Registrierung	608
35.1.2	Schritt 2: Zertifikate-Generierung	609
35.1.3	Schritt 3: PSE-Übergabe	610
35.1.4	Enrollment-Beispiele	610
35.1.5	Zertifizierungsanträge	614
35.2	Recovery	616
35.2.1	Schlüsselverlust-Problem	617
35.2.2	Chef-Sekretärin-Problem	618
35.2.3	Urlauber-Vertreter-Problem	619
35.2.4	Virens Scanner-Problem	620
35.2.5	Geht es auch ohne Recovery?	621
35.3	Abruf von Sperrinformationen	621
35.3.1	Sperrlisten	622

35.3.2	Online-Sperrprüfung	625
35.3.3	Weitere Formen des Abrufs von Sperrinformationen	627
36	Spezielle Fragen beim Betrieb einer PKI	631
36.1	Outsourcing oder Eigenbetrieb?	631
36.2	Gültigkeitsmodelle.	632
36.2.1	Schalenmodell	634
36.2.2	Kettenmodell.	635
36.3	Certificate Policy und CPS.	636
36.3.1	Was steht in einem CPS und einer Certification Policy? . . .	637
36.3.2	Nachteile von RFC 3647.	641
36.4	Policy-Hierarchien.	645
36.4.1	Hierarchietiefe.	645
36.4.2	Policy Mapping.	646
36.4.3	Policy-Hierarchien in der Praxis	647
37	Beispiel-PKIs	649
37.1	Signaturgesetze und dazugehörige PKIs	650
37.1.1	EU-Signaturrichtlinie.	650
37.1.2	Deutsches Signaturgesetz.	651
37.1.3	Österreichisches Signaturgesetz	654
37.1.4	Schweizer ZertES	654
37.1.5	Fazit	655
37.2	Die PKIs elektronischer Ausweise	655
37.2.1	Die PKI des elektronischen Reisepasses	655
37.2.2	PKIs elektronischer Personalausweise	656
37.2.3	PKIs elektronischer Krankenversichertenkarten.	657
37.3	Weitere PKIs	658
37.3.1	Organisationsinterne PKIs.	658
37.3.2	Kommerzielle Trust Center	659
37.4	Übergreifende PKIs	660
37.4.1	European Bridge-CA	660
37.4.2	Verwaltungs-PKI.	660
37.4.3	Wurzel-CAs.	661
37.5	Gehackte Zertifizierungsstellen	662
37.5.1	Comodo	662
37.5.2	DigiNotar	662
37.5.3	TurkTrust	663
37.5.4	Weitere Fälle	663

Teil 5

Kryptografische Netzwerkprotokolle

38	Kryptografie im OSI-Modell	667
38.1	Das OSI-Modell	668
38.1.1	Die Schichten des OSI-Modells.	668
38.1.2	Die wichtigsten Netzwerkprotokolle im OSI-Modell	669
38.2	In welcher Schicht wird verschlüsselt?	671
38.2.1	Kryptografie in Schicht 7 (Anwendungsschicht)	671
38.2.2	Kryptografie in Schicht 4 (Transportschicht)	672
38.2.3	Schicht 3 (Vermittlungsschicht)	673
38.2.4	Schicht 2 (Sicherungsschicht)	674
38.2.5	Schicht 1 (Bit-Übertragungsschicht)	674
38.2.6	Fazit.	675
38.3	Design eines kryptografischen Netzwerkprotokolls	675
38.3.1	Initialisierungsroutine.	675
38.3.2	Datenaustauschroutine.	676
39	Kryptografie in OSI-Schicht 1	679
39.1	Krypto-Erweiterungen für ISDN.	679
39.2	Kryptografie im GSM-Standard	680
39.2.1	Wie GSM Kryptografie einsetzt	681
39.2.2	Sicherheit von GSM	682
39.3	Kryptografie im UMTS-Standard	684
39.3.1	Von UMTS verwendete Krypto-Verfahren	684
39.3.2	UMTS-Krypto-Protokolle.	685
39.4	LTE	688
40	Krypto-Standards für OSI-Schicht 2	689
40.1	Krypto-Erweiterungen für PPP	690
40.1.1	CHAP und MS-CHAP	691
40.1.2	EAP	691
40.1.3	ECP und MPPE	692
40.1.4	Virtuelle Private Netze in Schicht 2	692
40.2	Kryptografie im WLAN	695
40.2.1	WEP.	695
40.2.2	WPA	698
40.2.3	WPA2	700

40.3	Kryptografie für Bluetooth	700
40.3.1	Grundlagen der Bluetooth-Kryptografie	701
40.3.2	Bluetooth-Authentifizierung und -Verschlüsselung	705
40.3.3	Angriffe auf die Bluetooth-Sicherheitsarchitektur	706
41	IPsec (Schicht 3)	709
41.1	Bestandteile von IPsec	710
41.1.1	ESP	710
41.1.2	AH	711
41.2	IKE	712
41.2.1	ISAKMP	712
41.2.2	Wie IKE ISAKMP nutzt.	714
41.2.3	IKEv2	716
41.3	Kritik an IPsec	716
41.4	Virtuelle Private Netze mit IPsec	717
42	TLS und DTLS (Schicht 4)	719
42.1	Funktionsweise von TLS	720
42.2	TLS-Protokollablauf	722
42.2.1	Das Record-Protokoll	722
42.2.2	Das Handshake-Protokoll	722
42.2.3	Das ChangeCipherSpec-Protokoll	723
42.2.4	Das Alert-Protokoll	723
42.2.5	Das ApplicationData-Protokoll	723
42.3	DTLS	724
42.4	TLS in der Praxis	724
42.5	Sicherheit von TLS	725
42.5.1	Angriffe auf TLS-Zertifikate	725
42.5.2	Der Heartbleed-Bug	725
42.5.3	FREAK und Logjam	725
42.5.4	Wie ist die Sicherheit von TLS einzuschätzen?	726
42.6	Vergleich zwischen IPsec und TLS	727
42.6.1	Webportal mit TLS oder VPN?	727
42.6.2	VPNs mit TLS	729
43	E-Mail-Verschlüsselung- und Signierung (Schicht 7)	731
43.1	Wie E-Mail funktioniert	731
43.2	Kryptografie für E-Mails	732
43.2.1	Clientbasierte E-Mail-Absicherung	733
43.2.2	Serverbasierte E-Mail-Absicherung	734
43.2.3	Versandportale	736

43.3	S/MIME	737
43.3.1	S/MIME-Format.	737
43.3.2	S/MIME-Profil von Common PKI	738
43.3.3	Bewertung von S/MIME.	739
43.4	OpenPGP	739
43.4.1	OpenPGP.	740
43.4.2	Bewertung von OpenPGP.	740
43.5	Abholen von E-Mails: POP und IMAP	741
43.5.1	Gefahren beim Abholen von E-Mails	741
43.5.2	Krypto-Zusätze für IMAP	742
43.5.3	Krypto-Zusätze für POP.	743
43.6	Die Krise der E-Mail-Verschlüsselung.	743
44	Weitere Krypto-Protokolle der Anwendungsschicht	747
44.1	Kryptografie im World Wide Web	747
44.1.1	Authentifizierung im World Wide Web	748
44.1.2	HTTP über TLS (HTTPS)	749
44.1.3	Web Cryptography API	751
44.2	Kryptografie für Echtzeitdaten im Internet (RTP)	752
44.2.1	SRTP	752
44.2.2	SRTP-Initialisierungsroutinen.	753
44.2.3	Bewertung von SRTP	755
44.3	Secure Shell (SSH).	755
44.3.1	Entstehungsgeschichte der Secure Shell.	756
44.3.2	Funktionsweise der Secure Shell	756
44.3.3	Bewertung der Secure Shell.	760
44.4	Online-Banking mit FinTS	760
44.4.1	Der Standard	761
44.4.2	Bewertung von FinTS.	763
44.5	Weitere Krypto-Protokolle in Schicht 7	763
44.5.1	Krypto-Erweiterungen für SNMP.	763
44.5.2	DNSSEC und TSIG	764
44.5.3	Kryptografie für SAP R/3	767
44.5.4	Verschlüsselte Kurznachrichten	768
44.5.5	SASL	769
44.5.6	Sicheres NTP und sicheres SNTP	770

45	Digitales Bezahlen	771
45.1	EMV	772
45.1.1	Kryptografische Mechanismen von EMV	773
45.1.2	Bewertung von EMV	775
45.2	Bezahlkarten	775
45.3	Online-Bezahlsysteme	777
45.3.1	Arten von Online-Bezahlsystemen	777
45.4	Bitcoin	781
45.4.1	Funktionsweise von Bitcoin	781
45.4.2	Bitcoin in der Praxis	783
46	Noch mehr Kryptografie in der Anwendungsschicht	785
46.1	Dateiverschlüsselung	785
46.2	Festplattenverschlüsselung	787
46.3	Code Signing	789
46.4	Versandportale	790
46.5	Elektronische Ausweise	791
46.5.1	Elektronische Reisepässe	792
46.5.2	Elektronische Personalausweise	793
46.5.3	Elektronische Gesundheitskarten	794
46.5.4	Weitere elektronische Ausweise	795
46.6	Digital Rights Management	795
46.6.1	Containment und Marking	796
46.6.2	Beispiele für DRM-Systeme	798
46.7	Smart Metering und Smart Grids	801
46.7.1	Der SMGW-Standard	802
46.7.2	OSGP	803
46.8	Elektronische Wahlen und Online-Wahlen	803

Teil 6

Mehr über Kryptografie

47	Wo Sie mehr zum Thema erfahren	807
47.1	Buchtipps	807
47.2	Veranstaltungen zum Thema Kryptografie	813
47.3	Zeitschriften zum Thema Kryptografie	816
47.4	Weitere Informationsquellen	817
47.4.2	Museen	817
47.4.3	Software	818

48	Kryptografisches Sammelsurium	821
48.1	Die zehn wichtigsten Personen der Kryptografie	821
48.1.1	Vater der Kryptografie: William Friedman (1891–1969) ..	822
48.1.2	Begründer der Krypto-Geschichte: David Kahn (*1930) ..	823
48.1.3	Guru und Rebell: Whitfield Diffie (*1944)	824
48.1.4	Der Pionier: Martin Hellman (*1946)	825
48.1.5	Der bedeutendste Kryptograf der Gegenwart: Ron Rivest (*1947)	825
48.1.6	Deutschlands bester Codeknacker: Hans Dobbertin (1952–2006)	826
48.1.7	Das »S« in RSA: Adi Shamir (*1952)	827
48.1.8	Der Volksheld: Phil Zimmermann (*1954)	828
48.1.9	Der Krypto-Papst: Bruce Schneier (*1963)	829
48.1.10	Zweifacher Wettbewerbssieger: Joan Daemen (*1965) . . .	830
48.2	Die wichtigsten Unternehmen	831
48.2.1	Applied Security	831
48.2.3	Crypto AG	832
48.2.4	cryptovision	832
48.2.5	CryptWare	833
48.2.6	Entrust Technologies	833
48.2.7	Rohde & Schwarz SIT	833
48.2.8	RSA Security	833
48.2.9	Secude	834
48.2.10	Secunet	834
48.2.11	Secusmart	834
48.2.12	Sirrix	835
48.2.13	Utimaco	835
48.2.14	Wibu Systems	835
48.2.15	Zertificon	835
48.3	Non-Profit-Organisationen	836
48.3.1	BSI	836
48.3.2	Bundesnetzagentur	836
48.4	Kryptoanalyse-Wettbewerbe	839
48.4.1	Die RSA-Challenges	839
48.5	Die zehn größten Krypto-Flops	843
48.5.7	Der Heartbleed-Bug	847
48.6	Murphys zehn Gesetze der Kryptografie	849

Anhang

Bildnachweis	853
Literatur	855
Index	883